**Best practices for securely storing API keys**

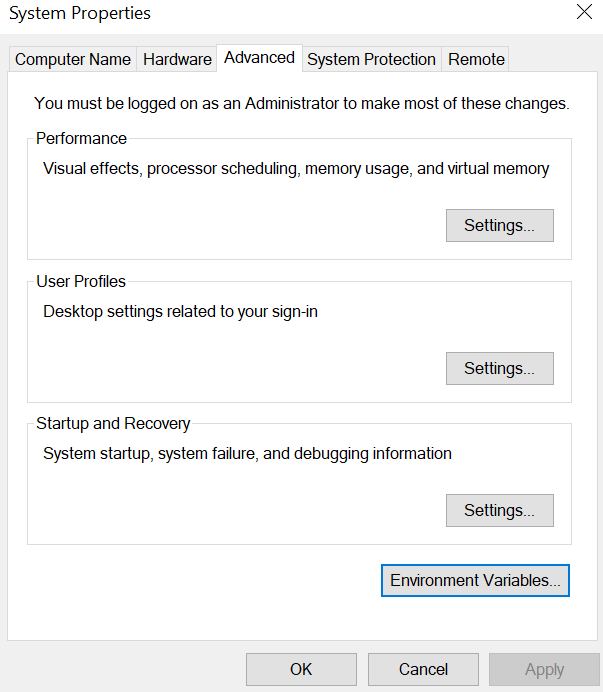
Storing API Keys, or any other sensitive information like Database name/password, on a git repository is something to be avoided at all costs.

**So, where should API keys be stored?**

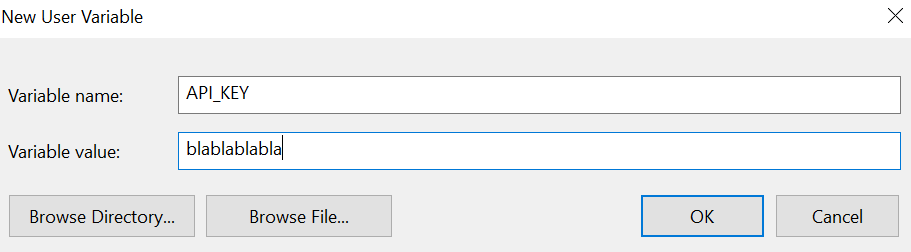
There are many alternatives for securely storing API keys and secrets and one of them is environment variable. An environment variable’s value is set outside the program, typically through a functionality built into the operating system. Also, environment variables provide a greater degree of flexibility for switching between local development setup and [production setup](https://djangocentral.com/deploy-django-with-nginx-gunicorn-postgresql-and-lets-encrypt-ssl-on-ubuntu/).

**Steps**

1. Create Environment variable for your API key



1. Give API key name(API\_KEY) and value



1. Settings.py – Store environment variable value in settings.py



1. Views.py   
   *import settings ->* ***from django.conf import settings***

***Set API key in context and pass it to template***

context={ 'API\_KEY':settings.MY\_API\_KEY }

1. *Now you can access api key in Templates*

***<script async defer src="https://maps.googleapis.com/maps/api/js?key={{API\_KEY}}&libraries=places&callback=initMap">***

***</script>***